(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－257670
（Ｐ２００１－２５７６７０Ａ）
(43)公開日　平成13年９月21日(2001.9.21)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
H04L 9/10		G06F 12/14	320	B	5B017
G06F 12/14	320	15/00	330	Z	5B058
15/00	330	17/30	120	B	5B075
17/30	120	G06K 17/00		T	5B085
G06K 17/00		G09C 1/00	660	A	5C053

審査請求　未請求　請求項の数４　ＯＬ　（全14頁）　最終頁に続く

(21)出願番号　特願2000－70671(Ｐ2000－70671)

(22)出願日　平成12年３月14日(2000.3.14)

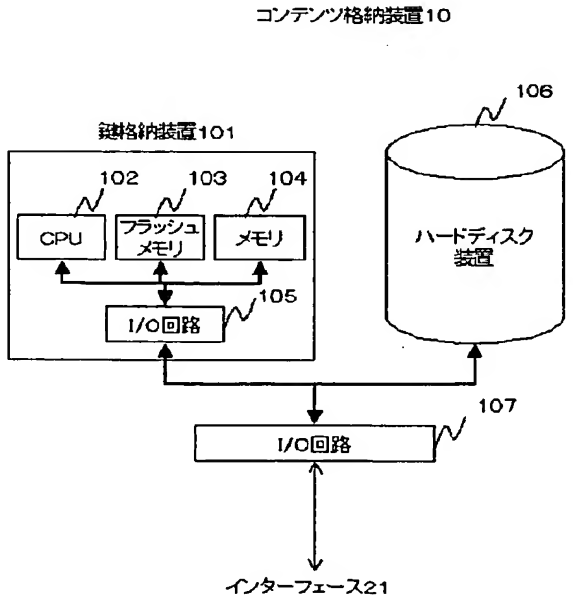
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　常広　隆司
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　片山　国弘
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100087170
弁理士　富田　和子

最終頁に続く

(54)【発明の名称】コンテンツ記憶装置およびコンテンツ読取装置

(57)【要約】
【課題】コンテンツ著作者などの保護を図りつつも、大量のコンテンツデータを取り扱えるようにする。
【解決手段】コンテンツデータ毎に用意されたライセンス鍵は、暗号化されたコンテンツデータを格納するハードディスク装置１０６とは別個に設けられた鍵格納装置１０１に格納する。鍵格納装置１４は通信相手の認証機能を有し、当該機能により再生装置が通信相手として認証された場合は、暗号通信を利用して当該再生装置に再生対象コンテンツデータに対応するライセンス鍵を送信する。メモリカードが通信相手として認証された場合は、暗号通信を利用して当該要求対象のライセンス鍵を送信するとともに、送信したライセンス鍵を記憶内容から消去する。

図2



1

【特許請求の範囲】

【請求項１】暗号化されたコンテンツデータを記憶するコンテンツ記憶装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、前記コンテンツ格納手段とは別個に設けられた計算機能付き鍵格納手段と、を有し前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、

前記認証手段によりコンテンツデータの再生装置が通信相手として認証された場合に、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記認証手段により他の記憶装置が通信相手として認証された場合に、暗号通信を利用して、当該他の記憶装置へ送信すべき鍵を読み出して当該他の記憶装置へ送信するとともに、送信した鍵を記憶内容から消去することを特徴とするコンテンツ記憶装置。

【請求項２】請求項１記載のコンテンツ記憶装置であって、

前記計算機能付き鍵格納手段は、

本コンテンツ記憶装置に装着自在に構成されていることを特徴とするコンテンツ記憶装置。

【請求項３】暗号化されたコンテンツデータが記憶された可搬性を有する記憶媒体から、コンテンツデータを読み取るコンテンツ読取装置であって、

前記記憶媒体から暗号化されたコンテンツデータを読み取るコンテンツ読取手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納手段と、を有し前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、

前記認証手段によりコンテンツデータの再生装置が通信相手として認証された場合に、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記認証手段により他の記憶装置が通信相手として認証された場合に、暗号通信を利用して、当該他の記憶装置へ送信すべき鍵を読み出して当該他の記憶装置へ送信するとともに、送信した鍵を記憶内容から消去することを特徴とするコンテンツ読取装置。

【請求項４】請求項３記載のコンテンツ読取装置であって、

前記計算機能付き鍵格納手段は、

本コンテンツ読取装置に装着自在に構成されていることを特徴とするコンテンツ読取装置。

【発明の詳細な説明】

2

【０００１】

【発明の属する技術分野】本発明は、正当な権利者のみに、オーディオデータやビデオデータなどのコンテンツデータの利用を許可する技術に関し、特に、大量のコンテンツデータを取り扱うのに好適なコンテンツ記憶装置およびコンテンツ読取装置に関する。

【０００２】

【従来の技術】近年、オーディオデータやビデオデータなどのコンテンツデータをネットワークを介して配信しようとする試みがなされている。たとえば、専用のメモリカードを用意し、これを販売店などに設置された専用端末に装着し、オンラインシステムを利用して所望のコンテンツデータを前記メモリカード内にダウンロードする。あるいは、専用のメモリカードを携帯電話等の個人向け端末に装着し、インターネットを利用して、コンテンツ配信センタから前記メモリカード内にダウンロードする。コンテンツデータを再生する場合には、コンテンツデータを格納した前記メモリカードを専用の再生装置に装着し、再生する。

【０００３】

【発明が解決しようとする課題】さて、上述のような専用のメモリカードには、コンテンツデータの複製が容易であることから、コピー防止機能を設けるなどしてコンテンツ著作者などの保護を図る必要がある。

【０００４】しかしながら、メモリカードでは、容量に限界があるため、大量のコンテンツデータを保存することができない。ユーザは、現在利用していないコンテンツデータであっても、コレクションとしてとっておきたい場合がある。この場合、メモリカードにコピー防止機能が付加されていると、ユーザは、メモリカードがコンテンツデータで満杯になる都度、新たなメモリカードを購入しなければならず、経済的な負担が大きい。

【０００５】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、コンテンツ著作者などの保護を図りつつも、大量のコンテンツデータを取り扱うことが可能なコンテンツ記憶装置およびコンテンツ読取装置を提供することにある。

【０００６】

【課題を解決するための手段】上記課題を解決するために、本発明では、コンテンツデータもしくは当該データのグループ毎に異なる鍵で暗号化されたコンテンツデータをたとえばＨＤＤなどのコンテンツ格納手段、あるいは、ＣＤなどの可搬性を有する記憶媒体に記憶する。そして、コンテンツデータもしくは当該データのグループ毎に用意された、暗号化されたコンテンツデータを復号するための鍵は、コンテンツ格納手段や記憶媒体とは別個に設けられた計算機能付き格納手段に格納しておく。

【０００７】ここで、計算機能付き鍵格納手段は、通信相手を認証する認証手段を有し、当該認証手段によりコンテンツデータの再生装置が通信相手として認証された

場合は、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信する。また、当該認証手段により他の記憶装置が通信相手として認証された場合は、暗号通信を利用して、当該他の記憶装置へ送信すべき鍵を読み出して当該他の記憶装置へ送信するとともに、送信した鍵を記憶内容から消去する。

【０００８】本発明において、コンテンツ格納手段あるいは可搬性を有する記憶媒体に格納されたコンテンツデータは暗号化されているので、対応する鍵がなければ復号し利用することができない。したがって、コンテンツ格納手段や記憶媒体あるいは当該媒体の読取手段に、コピー防止機能といった特別な機能を設ける必要がなくなるため、コンテンツ格納手段として一般に市販されている大容量のハードディスク装置などを利用したり、あるいは、コンテンツ読取手段として一般に市販されているＣＤ読取装置などを利用したりすることができる。このため、大量のコンテンツデータを格納することが可能となる。

【０００９】また、コンテンツ格納手段や記憶媒体に格納されたコンテンツデータを復号するためには対応する鍵が必要となるため、この鍵が計算機能付き鍵格納手段に格納されていなければ、当該コンテンツデータを復号することができない。したがって、正当な権利者（対応する鍵を有する者）のみに、コンテンツデータの再生を許可することができ、コンテンツ著作者などの保護を図ることができる。

【００１０】さらに、本発明では、計算機能付き鍵格納手段に認証手段を設けている。そして、コンテンツデータの再生装置が通信相手として認証された場合、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信している。つまり、暗号化されたコンテンツデータの復号を再生装置側で行わせるようにしている。このようにすることで、鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。また、他の記憶装置が通信相手として認証された場合は、送信対象の鍵を当該他の記憶装置に送信するとともに、送信した鍵を記憶内容から消去している。このようにすることで、鍵が不正にコピーされる可能性をより低くすることができ、セキュリティを向上できる。

【００１１】なお、一般に、暗号化されたコンテンツデータを復号するための鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、計算機能付き鍵格納手段として、本コンテンツ記憶装置あるいは読取装置に装着自在に構成された、従来の技術で説明したようなコピー防止機能を備えたメモリカードを用いた場合でも、当該メモリカードに大量のコンテンツデータに対応する鍵を格納することができるので、大量のコンテンツデータを、そのコンテンツデータを復号する鍵とともに取り扱うことが可能となる。

【００１２】

【発明の実施の形態】以下に、本発明の１実施形態について説明する。

【００１３】図１は、本発明の１実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

【００１４】図１において、コンテンツ格納装置１０には、暗号化されたオーディオデータやビデオデータなどのコンテンツデータがそのコンテンツ名称に対応付けられて格納される。また、コンテンツ毎に用意された、暗号化されたコンテンツデータを復号するための鍵（以下、ライセンス鍵と称する）が格納される。

【００１５】ＣＰＵ１１は、コンテンツ再生装置の各部を統括的に制御する。メモリ１２は、ＲＯＭおよびＲＡＭから構成される。ＲＯＭには、ＣＰＵ１１が本コンテンツ再生装置の各部を統括的に制御するためのプログラムが格納されている。ＲＡＭは、ＣＰＵ１１のワークエリアとして機能する。

【００１６】通信装置１５は、携帯電話機や据置型の電話機に接続し、オンラインシステムやインターネットなどのネットワークを介して、たとえば暗号化されたコンテンツデータやライセンス鍵を配信するコンテンツ配信センタ（不図示）にアクセスし、暗号化されたコンテンツデータやライセンス鍵を入手するのに用いられる。

【００１７】入力装置１６は、たとえば各種ボタンやタッチパネルで構成され、ユーザからの再生指示やコンテンツデータ、ライセンス鍵の入手指示を受け付ける。

【００１８】表示装置１７は、たとえば液晶パネルで構成され、コンテンツ格納装置１０に格納されている暗号化されたコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。

【００１９】オーディオ再生装置１８は、コンテンツ格納装置１０のなかから再生対象の暗号化されたオーディオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、オーディオ信号を得る。そして、オーディオ信号を本コンテンツ再生装置に接続されたステレオに出力する。ビデオ再生装置１９は、コンテンツ格納装置１０のなかから再生対象の暗号化されたビデオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、ビデオ信号を得る。そして、ビデオ信号を本コンテンツ再生装置に接続されたモニタに出力する。

【００２０】カード接続装置２０は、メモリカード３０を接続し、当該メモリカード３０から暗号化されたコンテンツデータやライセンス鍵を入手したり、当該メモリカード２０へ暗号化されたコンテンツデータやライセンス鍵を送ったりする。

【００２１】インターフェース２１は、ＣＰＵ１１やメ

モリ１２と本コンテンツ再生装置を構成する他装置との間のデータ送受を司る。

【００２２】次に、本コンテンツ再生装置を構成する各装置のうち、コンテンツ格納装置１０、オーディオ再生装置１８およびビデオ再生装置１９について、さらに詳細に説明する。

【００２３】まず、コンテンツ格納装置１０について説明する。

【００２４】図２は、コンテンツ格納装置１０の概略構成を示す図である。

【００２５】図示するように、コンテンツ格納装置１０は、ハードディスク装置１０６と、鍵格納装置１０１と、ハードディスク装置１０６および鍵格納装置１０１がインターフェース２１を介して本コンテンツ再生装置の各部とデータ送受を行うためのＩ/Ｏ回路１０７と、を備えて構成される。

【００２６】ハードディスク装置１０には、暗号化されたオーディオデータやビデオデータなどのコンテンツデータがそのコンテンツ名称に対応付けられて格納される。

【００２７】鍵格納装置１０１は、ＣＰＵ１０２と、メモリ１０４と、フラッシュメモリ１０３と、Ｉ/Ｏ回路１０７とのインターフェースであるＩ/Ｏ回路１０５と、を有する。

【００２８】ＣＰＵ１０２は、鍵格納装置１０１の各部を統括的に制御する。また、ＣＰＵ１０２は、認証機能と暗復号化機能を有している。メモリ１０４は、ＲＯＭおよびＲＡＭから構成される。ＲＯＭには、ＣＰＵ１０２が鍵格納装置１０１の各部を統括的に制御するためのプログラムと、認証機能および暗復号化機能を実現するためのプログラムが格納されている。ＲＡＭは、ＣＰＵ１０２のワークエリアとして機能する。フラッシュメモリ１０３には、ライセンス鍵が復号対象コンテンツのコンテンツ名称に対応付けられて格納される。ここで、ライセンス鍵は、セキュリティをより強固にするため、いわゆるタンパ・レジスタント領域（TRM:Tamper Resistant Module）に格納するのがよい。なお、フラッシュメモリ１０３の代わりに、ＦＲＡＭやＥＥＰＲＯＭなどのその他の不揮発性メモリを用いることができる。

【００２９】図２に示す鍵格納装置１０１を構成する各部は、たとえば１チップ上につくり込まれるようにしてもよいし、あるいは、複数チップで構成されるようにしてもよい。複数チップで構成する場合は、鍵格納装置１０１の外部からチップ間の信号を盗み取られないような工夫を施すことが好ましい。

【００３０】なお、図２に示す鍵格納装置１０１を構成する各部は、たとえば１チップ上につくり込まれる。

【００３１】次に、オーディオ再生装置１８について説明する。

【００３２】図３は、オーディオ再生装置１８の概略構成を示す図である。

【００３３】図示するように、オーディオ再生装置１８は、暗復号化回路１８１と、デコーダ回路１８２と、インターフェース２１を介して本コンテンツ再生装置の各部とデータ送受を行うためのＩ/Ｏ回路１８４と、を有する。

【００３４】暗復号化回路１８１は、コンテンツ格納装置１０の鍵格納装置１０１から再生対象の暗号化されたオーディオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置１０のハードディスク装置１０６から読み出された再生対象の暗号化されたオーディオデータを復号する。デコーダ回路１８２は、暗復号化回路１８１で復号化されたオーディオデータを、必要に応じて伸長し、再生して、オーディオ信号を得る。そして、オーディオ信号をステレオに出力する。ここで、図３に示すオーディオ再生装置１８を構成する各部は、たとえば１チップ上につくり込まれる。

【００３５】次に、ビデオ再生装置１９について説明する。

【００３６】図４は、ビデオ再生装置１９の概略構成を示す図である。

【００３７】図示するように、ビデオ再生装置１９は、暗復号化回路１９１と、デコーダ回路１９２と、フレームバッファ１９３と、インターフェース２１を介して本コンテンツ再生装置の各部とデータ送受を行うためのＩ/Ｏ回路１９４とを有する。

【００３８】暗復号化回路１９１は、コンテンツ格納装置１０の鍵格納装置１０１から再生対象の暗号化されたビデオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置１０のハードディスク装置１０６から読み出された再生対象の暗号化されたビデオデータを復号する。デコーダ回路１８２は、フレームバッファ１９３を利用して、暗復号化回路１８１で復号化されたビデオデータを、必要に応じて伸長し、再生して、ビデオ信号を得る。そして、ビデオ信号をモニタに出力する。ここで、図４に示すビデオ再生装置１９を構成する各部は、たとえば１チップ上につくり込まれる。

【００３９】次に、本コンテンツ再生装置に装着されて用いられるメモリカード３０について説明する。

【００４０】メモリカード３０の概略構成は、図２に示すコンテンツ格納装置１０の鍵格納装置１０１と同じである。ただし、メモリカード３０には、ライセンス鍵のみならず、暗号化されたコンテンツデータも格納されるものとする。すなわち、このメモリカード３０は、たとえば販売店などに設置された専用端末に装着されて、ユーザがオンラインシステムを利用して所望の暗号化されたコンテンツデータやそのライセンス鍵を入手したり、あるいは、携帯電話等の個人向け端末に装着されて、ユーザがインターネットを利用してコンテンツ配信センタから所望の暗号化されたコンテンツデータやそのライセ

ンス鍵を入手したりするのに用いることができるものとする。

【００４１】ここで、図５に、本実施形態が適用されたコンテンツ再生装置の概観の一例を示す。この例のコンテンツ再生装置は、家庭内でコンテンツを楽しむのに適した据置型の形状をしている。ここで、符号４１は、再生ボタン、停止ボタン、再生コンテンツ選択ボタン、および、コンテンツデータやライセンス鍵をコンテンツ格納装置１０のハードディスク装置１０６や鍵格納装置１０１へ書き込んだり、カード接続装置３０に接続されたメモリカード２０へ移動したりするための各種設定ボタンなどで構成される操作パネルである。符号４２は、操作パネル４１と同じ各種ボタンを備えたリモコン５０からの指示を受け付けるための受信部である。符号４３は、表示パネルであり、コンテンツ格納装置１０のハードディスク装置１０６に格納されているコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。そして、符号４４は、メモリカード３０を装着するためのスロットである。図示していないが、本コンテンツ装置の背面には、モニタ５１やステレオ５２や携帯電話機５３あるいは電話機を接続するための端子が設けられている。

【００４２】次に、図６に、コンテンツ記憶装置１０の概観の一例を示す。この例のコンテンツ記憶装置１０は、ハードディスク装置１０６に鍵格納装置１０１を装着するためのスロットが設けられた形状をしている。ここで、符号４６は、本コンテンツ格納装置１０をコンテンツ再生装置のケーブル４７に接続するためのコネクタであり、コンテンツ再生装置が採用するインターフェースに準拠している。符号４５は、鍵格納装置１０１を装着するためのスロットである。鍵格納装置１０１には、たとえばメモリカード３０と同じ構成のものを用いることができる。

【００４３】なお、図５に例示するコンテンツ再生装置では、コンテンツ格納装置１０を筐体内部に内蔵し、ユーザ自身が鍵格納装置１０１を挿抜できないようにしている。しかし、ユーザ自身がコンテンツ格納装置１０の鍵格納装置１０を挿抜できるように、コンテンツ格納装置１０のスロット４５がコンテンツ再生装置の筐体の面上にくるようにしてもかまわない。あるいは、コンテンツ格納装置１０自体を挿抜できるようにするために、コンテンツ再生装置にコンテンツ格納装置１０を装着するためのスロットを設けるようにしてもかまわない。

【００４４】また、図６に例示するコンテンツ格納装置１０では、鍵格納装置１０１を挿抜できるようにスロット４５を設けているが、たとえば鍵格納装置１０１をコンテンツ格納装置１０の内部に組み込んで、挿抜できないようにしてもかまわない。たとえば、鍵格納装置１０１をＩＣやＬＳＩと同じ形状のものとし、これをコンテンツ格納装置１０内部の基板上に設けられたソケットへ取り付けるようにしてもかまわない。あるいは、これをコンテンツ格納装置１０内部の基板に直接半田付けするようにしてもかまわない。

【００４５】次に、本実施形態のコンテンツ再生装置の動作について説明する。

【００４６】まず、コンテンツデータを再生する場合の動作について説明する。

【００４７】図７は、本実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。このフローは、たとえば、ユーザが入力装置１６を用いて、表示装置１７に表示されている、コンテンツ格納装置１０のハードディスク装置１０６に格納されているコンテンツデータのコンテンツ名称のリストのなかから、再生対象のコンテンツを選択し、再生指示を入力すると開始される。

【００４８】まず、ＣＰＵ１１は、入力装置１６を介してユーザより受け付けたコンテンツデータの再生指示を、当該コンテンツデータの種類（オーディオデータ/ビデオデータ）を再生するオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｓ１００１）。

【００４９】ＣＰＵ１１より再生指示を受け取ったオーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、自身の認証データと再生対象の暗号化されたコンテンツデータの識別情報（たとえばコンテンツ名称）を含んだ、当該コンテンツデータ再生のためのライセンス鍵送信指示を、コンテンツ格納装置１０の鍵格納装置１０１に送信する（Ｓ１００２）。

【００５０】鍵格納装置１０１のＣＰＵ１０２は、コンテンツデータ再生のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（Ｓ１００３）。たとえば、認証データが予め本鍵格納装置１０１に登録されているオーディオ/ビデオ再生装置であることを示しているか否かを調べる。そして、当該指示の送信元がオーディオ再生装置１８/ビデオ再生装置１９であることを認証したならば（Ｓ１００４でＹｅｓの場合）、当該指示に含まれる識別情報により特定されるコンテンツデータのライセンス鍵がフラッシュメモリ１０３に格納されているか否かを調べる（Ｓ１００５）。格納されていれば（Ｓ１００６でＹｅｓの場合）、そのライセンス鍵をフラッシュメモリ１０３から読み出し、暗号通信を利用して、当該指示の送信元であるオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｓ１００８）。

【００５１】なお、Ｓ１００４において指示の送信元がオーディオ再生装置１８/ビデオ再生装置１９であることを認証できなかった場合、および、Ｓ１００６において所望のライセンス鍵がフラッシュメモリ１０３に格納されていなかった場合、鍵格納装置１０１のＣＰＵ１０２は、ＣＰＵ１１にその旨伝える。これを受けて、ＣＰ

Ｕ１１は表示装置１７にエラー表示を行うなど、所定のエラー処理を行う（Ｓ１００７）。

【００５２】さて、コンテンツデータ再生のためのライセンス鍵送信指示を送信したオーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、コンテンツ格納装置１０の鍵格納装置１０１からライセンス鍵を受け取ると、コンテンツ格納装置１０のハードディスク装置１０６から再生対象の暗号化されたコンテンツデータを読み出す（Ｓ１００９）。そして、これをライセンス鍵で復号して、デコーダ回路１８２/１９２に渡す。デコーダ回路１８２/１９２は、暗複号化回路１８１/１９１から受け取ったコンテンツデータを必要に応じて伸長し、再生してオーディオ/ビデオデータを得、ステレオ/モニタに出力する（Ｓ１０１０）。

【００５３】次に、図７に示すフローにおける鍵格納装置１０１およびオーディオ再生装置１８/ビデオ再生装置１９間のデータのやり取りについて、その一例を説明する。

【００５４】図８は、図７に示すフローにおける鍵格納装置１０１およびオーディオ再生装置１８/ビデオ再生装置１９間のデータのやり取りの一例を説明するためのシーケンス図である。

【００５５】オーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、図７のＳ１００２において、自身の認証データと、再生対象の暗号化されたコンテンツデータの識別情報と、予め保持しているメディアクラス秘密鍵K_{PMC}と対のメディアクラス公開鍵K_{OMC}とを含んだライセンス鍵送信指示を作成し、これをコンテンツ格納装置１０の鍵格納装置１０１に送信する（Ｔ１００１）。

【００５６】これを受けて、鍵格納装置１０１のＣＰＵ１０２は、図７のＳ１００４～Ｓ１００７において、オーディオ再生装置１８/ビデオ再生装置１９の認証、および、フラッシュメモリ１０３に要求されたライセンス鍵が格納されていることの確認を行う（Ｔ１００２）。それから、ＣＰＵ１０２は、セッション鍵K_{S1}を生成し（Ｔ１００３）、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵K_{OMC}で暗号化して、当該指示の送信元であるオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｔ１００４）。

【００５７】これを受けて、オーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、暗号化されたセッション鍵K_{S1}を予め保持しているメディアクラス秘密鍵K_{PMC}で復号し、セッション鍵K_{S1}を得る（Ｔ１００５）。それから、乱数K_{S2}を生成し（Ｔ１００６）、これと、予め保持しているメディア固有秘密鍵K_{PM}と対のメディア固有公開鍵K_{OM}とを、セッション鍵K_{S1}で暗号化して、コンテンツ格納装置１０の鍵格納装置１０１に送信する（Ｔ１００７）。

【００５８】これを受けて、鍵格納装置１０１のＣＰＵ１０２は、暗号化された乱数K_{S2}とメディア固有公開鍵K_{OM}を、セッション鍵K_{S1}で復号し、乱数K_{S2}とメディア固有公開鍵K_{OM}を得る（Ｔ１００８）。そして、送信を要求されているライセンス鍵K_Cをメディア固有公開鍵K_{OMC}で暗号化し、さらにこれを乱数K_{S2}で暗号化して、ライセンス鍵送信指示の送信元であるオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｔ１００９）。

【００５９】これを受けて、オーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、暗号化されたライセンス鍵K_Cを乱数K_{S2}とメディア固有秘密鍵K_{PM}を用いて復号し、ライセンス鍵K_Cを得る（Ｔ１０１０）。

【００６０】以上、コンテンツデータを再生する場合の動作について説明した。

【００６１】次に、メモリカード３０からライセンス鍵を入手する場合の動作について説明する。

【００６２】図９は、本実施形態が適用されたコンテンツ再生装置に接続されたメモリカード３０からライセンス鍵を入手する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード３０が装着された状態で、ユーザが入力装置１６を用いて、表示装置１７に表示されている、メモリカード３０に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、入手対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵入手指示を入力すると開始される。

【００６３】まず、ＣＰＵ１１は、入力装置１６を介してユーザよりライセンス鍵入手指示を受け付けたならば、その旨をコンテンツ格納装置の鍵格納装置１０１に送信する（Ｓ２００１）。

【００６４】ＣＰＵ１１よりライセンス鍵入手指示を受け取った鍵格納装置１０１のＣＰＵ１０２は、自身の認証データと入手対象のライセンス鍵の識別情報（たとえば当該鍵で復号可能なコンテンツ名称）を含んだ、当該ライセンス鍵入手のためのライセンス鍵送信指示を、カード接続装置２０に接続されたメモリカード３０に送信する（Ｓ２００２）。

【００６５】メモリカード３０のＣＰＵは、ライセンス鍵入手のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（Ｓ２００３）。たとえば、認証データが予め本メモリカード３０に登録されている鍵格納装置であることを示しているか否かを調べる。そして、当該指示の送信元が鍵格納装置１０１であることを認証したならば（Ｓ２００４でＹｅｓの場合）、当該指示に含まれる識別情報により特定されるライセンス鍵がメモリカード３０内に格納されているか否かを調べる（Ｓ２００５）。格納されていれば（Ｓ２００６でＹｅｓの場合）、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信

元であるコンテンツ格納装置１０の鍵格納装置１０１に送信する（Ｓ２００８）。それから、送信したライセンス鍵をメモリカード３０内から消去する（Ｓ２００９）。

【００６６】なお、Ｓ２００４において指示の送信元が鍵格納装置１０１であることを認証できなかった場合、および、Ｓ２００６において所望のライセンス鍵がメモリカード３０内に格納されていなかった場合、メモリカード３０のＣＰＵは、ＣＰＵ１１にその旨伝える。これを受けて、ＣＰＵ１１は表示装置１７にエラー表示を行うなど、所定のエラー処理を行う（Ｓ２００７）。

【００６７】さて、ライセンス鍵入手のためのライセンス鍵送信指示を送信した鍵格納装置１０１のＣＰＵ１０２は、カード接続装置２０に接続されたメモリカード３０からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてフラッシュメモリ１０３に格納する（Ｓ２０１０）。

【００６８】次に、図９に示すフローにおける鍵格納装置１０１およびメモリカード３０間のデータのやり取りについて、その一例を説明する。

【００６９】図１０は、図９に示すフローにおける鍵格納装置１０１およびメモリカード３０間のデータのやり取りの一例を説明するためのシーケンス図である。

【００７０】コンテンツ格納装置１０の鍵格納装置１０１のＣＰＵ１０２は、図９のＳ２００２において、自身の認証データと、入手対象のライセンス鍵の識別情報と、予め保持しているメディアクラス秘密鍵K'_{PMC}と対のメディアクラス公開鍵K'_{OMC}とを含んだライセンス鍵送信指示を作成し、これをメモリカード３０に送信する（Ｔ２００１）。

【００７１】これを受けて、メモリカード３０のＣＰＵは、図９のＳ２００４～Ｓ２００７において、鍵格納装置１０１の認証、および、メモリカード３０内に要求されたライセンス鍵が格納されていることの確認を行う（Ｔ２００２）。それから、メモリカード３０のＣＰＵは、セッション鍵K_{S1}を生成し（Ｔ２００３）、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵K'_{OMC}で暗号化して、当該指示の送信元であるコンテンツ格納装置１０の鍵格納装置１０１に送信する（Ｔ２００４）。

【００７２】これを受けて、鍵格納装置１０１のＣＰＵ１０２は、暗号化されたセッション鍵K_{S1}を予め保持しているメディアクラス秘密鍵K'_{PMC}で復号し、セッション鍵K_{S1}を得る（Ｔ２００５）。それから、乱数K_{S2}を生成し（Ｔ２００６）、これと、予め保持しているメディア固有秘密鍵K'_{PM}と対のメディア固有公開鍵K'_{OM}とを、セッション鍵K_{S1}で暗号化して、メモリカード３０に送信する（Ｔ２００７）。

【００７３】これを受けて、メモリカード３０のＣＰＵは、暗号化された乱数K_{S2}とメディア固有公開鍵K'_{OM}を、セッション鍵K_{S1}で復号し、乱数K_{S2}とメディア固有公開鍵K'_{OM}を得る（Ｔ２００８）。そして、送信を要求されているライセンス鍵K_Cをメディア固有公開鍵K'_{OMC}で暗号化し、さらにこれを乱数K'_{S2}で暗号化して、ライセンス鍵送信指示の送信元であるコンテンツ格納装置１０の鍵格納装置１０１に送信する（Ｔ２００９）。

【００７４】これを受けて、鍵格納装置１０１のＣＰＵ１０２は、暗号化されたライセンス鍵K_Cを乱数K_{S2}とメディア固有秘密鍵K'_{PM}を用いて復号し、ライセンス鍵K_Cを得る（Ｔ２０１０）。

【００７５】以上、メモリカード３０からライセンス鍵を入手する場合の動作について説明した。

【００７６】次に、コンテンツ格納装置１０の鍵格納装置１０１に格納されているライセンス鍵をメモリカード３０へ移動する場合の動作について説明する。

【００７７】図１１は、本実施形態が適用されたコンテンツ再生装置のコンテンツ格納装置１０の鍵格納装置１０１から、本コンテンツ再生装置に接続されたメモリカード３０へライセンス鍵を移動する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード３０が装着された状態で、ユーザが入力装置１６を用いて、表示装置１７に表示された、コンテンツ格納装置１０の鍵格納装置１０１に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、移動対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵移動指示を入力すると開始される。

【００７８】まず、ＣＰＵ１１は、入力装置１６を介してユーザよりライセンス鍵移動指示を受け付けたならば、その旨をメモリカード３０に送信する（Ｓ３００１）。

【００７９】ＣＰＵ１１よりライセンス鍵移動指示を受け取ったメモリカード３０のＣＰＵは、自身の認証データと移動対象のライセンス鍵の識別情報（たとえば当該鍵で復号可能なコンテンツ名称）を含んだ、当該ライセンス鍵移動のためのライセンス鍵送信指示を、コンテンツ格納装置１０の鍵格納装置１０１に送信する（Ｓ３００２）。

【００８０】鍵格納装置１０１のＣＰＵ１０２は、ライセンス鍵移動のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（Ｓ３００３）。たとえば、認証データが予め本鍵格納装置１０１に登録されているメモリカードであることを示しているか否かを調べる。そして、当該指示の送信元がメモリカード３０であることを認証したならば（Ｓ３００４でＹｅｓの場合）、当該指示に含まれる識別情報により特定されるライセンス鍵がフラッシュメモリ１０３内に格納されているか否かを調べる（Ｓ３００

５）。格納されていれば（Ｓ３００６でＹｅｓの場合）、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信元であるメモリカード３０に送信する（Ｓ３００８）。それから、送信したライセンス鍵をフラッシュメモリ１０３内から消去する（Ｓ３００９）。

【００８１】なお、Ｓ３００４において指示の送信元がメモリカード３０であることを認証できなかった場合、および、Ｓ３００６において所望のライセンス鍵がフラッシュメモリ１０３内に格納されていなかった場合、鍵格納装置１０１のＣＰＵ１０２は、ＣＰＵ１１にその旨伝える。これを受けて、ＣＰＵ１１は表示装置１７にエラー表示を行うなど、所定のエラー処理を行う（Ｓ３００７）。

【００８２】さて、ライセンス鍵移動のためのライセンス鍵送信指示を送信したメモリカード３０のＣＰＵは、鍵格納装置１０１からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてメモリカード３０内に格納する（Ｓ３０１０）。

【００８３】なお、図１１に示すフローにおける鍵格納装置１０１およびメモリカード３０間のデータのやり取りは、図１０に示すシーケンス図において、鍵格納装置１０１およびメモリカード３０の動作を互いに交換したものとなる。

【００８４】以上、メモリカード３０へライセンス鍵を移動する場合の動作について説明した。

【００８５】なお、通信装置１５に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ（不図示）からライセンス鍵を入手する場合の動作は、一般的な、ネットワークを介したデータダウンロードと同じものでよい。ただし、正当な権利を有する者のみがライセンス鍵を入手できるようにするために、コンテンツ格納装置１０の鍵格納装置１０１とコンテンツ配信センタとの間で認証処理を行い、コンテンツ配信センタが鍵格納装置１０１を認証した場合にのみ、ライセンス鍵のダウンロードを許可するようにすることが好ましい。また、コンテンツデータのコンテンツ格納装置１０のハードディスク装置１０６へのダウンロードは、たとえば、メモリカード３０に格納されたコンテンツデータをコピーしてハードディスク装置１０６に格納するようにしてもよいし、あるいは、通信装置１５に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ（不図示）から入手し、ハードディスク装置１０６に格納するようにしてもよい。いずれにしても、コンテンツデータは暗号化されており、対応するライセンス鍵がなければ復号・再生できない。

【００８６】以上、本発明の１実施形態について説明した。

【００８７】本実施形態において、コンテンツ格納装置１０のハードディスク装置１０６に格納されたコンテンツデータは暗号化されているので、対応するライセンス鍵がなければ復号し再生することができない。したがって、ハードディスク装置１０６にコピー防止機能といった特別な機能を設ける必要がなくなるため、ハードディスク装置１０６として、一般に市販されている大容量のハードディスクドライブを利用でき、大量のコンテンツデータを格納することが可能となる。

【００８８】また、コンテンツ格納装置１０のハードディスク装置１０６に格納されたコンテンツデータを復号するためには対応するライセンス鍵が必要となるため、このライセンス鍵がコンテンツ格納装置１０の鍵格納装置１０１に格納されていなければ、当該コンテンツデータを再生することができない。したがって、正当な権利者（対応するライセンス鍵を有する者）のみに、コンテンツデータの再生を許可することができ、コンテンツ著作者などの保護を図ることができる。

【００８９】さらに、本実施形態では、暗号化されたコンテンツデータの復号を、コンテンツデータの再生を行うオーディオ再生装置１８/ビデオ再生装置１９で行うようにしている。そして、コンテンツ格納装置１０の鍵格納装置１０１は、ライセンス鍵の送信相手がオーディオ再生装置１８/ビデオ再生装置１であることを認証した場合に、当該ライセンス鍵を暗号通信を利用してオーディオ再生装置１８/ビデオ再生装置１９に送るようにしている。このようにすることで、ライセンス鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。

【００９０】くわえて、本実施形態において、コンテンツ格納装置１０の鍵格納装置１０１は、ライセンス鍵の送信相手がメモリカード３０である場合、送信したライセンス鍵を鍵格納装置１０１の記憶内容から消去するようにしている。つまり、鍵格納装置１０１にライセンス鍵のコピー防止機能を設けている。このようにすることで、ライセンス鍵が不正にコピーされる可能性を減らすことができる。

【００９１】なお、一般に、鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、鍵格納装置１０１の記憶部をフラッシュメモリ１０３で構成した場合でも、当該フラッシュメモリ１０３に多くのライセンス鍵を格納することができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

【００９２】なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【００９３】たとえば、上記の実施形態では、暗号化されたコンテンツデータがコンテンツ格納装置１０のハードディスク装置１０６に格納されている場合を例に取り説明した。しかしながら、本発明はこれに限定されるものではない。暗号化されたコンテンツデータは、ＣＤなどの可搬性を有する記憶媒体に格納された形態で提供されるものでもよい。この場合、本実施形態において、コンテンツ格納装置１０のハードディスク装置１０６に代えて、前記可搬性を有する記憶媒体から暗号化されたコンテンツデータを読み取る読取装置を設けるようにすればよい。

【００９４】また、、上記の実施形態では、ライセンス鍵を暗号化されたコンテンツデータ毎に用意しているが、本発明はこれに限定されない。たとえば、複数の暗号化されたコンテンツデータを１グループとして、グループ毎に、当該グループに属する暗号化されたコンテンツデータを復号するためのライセンス鍵を用意するようにしてもよい。

【００９５】

【発明の効果】以上説明したように、本発明によれば、コンテンツ著作者などの保護を図りつつも、大量のコンテンツデータを取り扱うことが可能となる。

【図面の簡単な説明】

【図１】本発明の１実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

【図２】図１に示すコンテンツ格納装置１０の概略構成を示す図である。

【図３】図１に示すオーディオ再生装置１８の概略構成を示す図である。

【図４】図１に示すビデオ再生装置１９の概略構成を示す図である。

【図５】本発明の１実施形態が適用されたコンテンツ再生装置の概観の一例を示す図である。

【図６】図２に示すコンテンツ格納装置１０の概観の一例を示す図である。

【図７】本発明の第１実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。

【図８】図７に示すフローにおけるコンテンツ格納装置１０の鍵格納装置１０１およびオーディオ再生装置１８/ビデオ再生装置１９間のデータのやり取りの一例を説明するためのシーケンス図である。

【図９】本発明の第１実施形態が適用されたコンテンツ再生装置に接続されたメモリカード３０からライセンス鍵を入手する場合の動作を説明するためのフロー図である。

【図１０】図９に示すフローにおけるコンテンツ格納装置１０の鍵格納装置１０１およびメモリカード３０間のデータのやり取りの一例を説明するためのシーケンス図である。

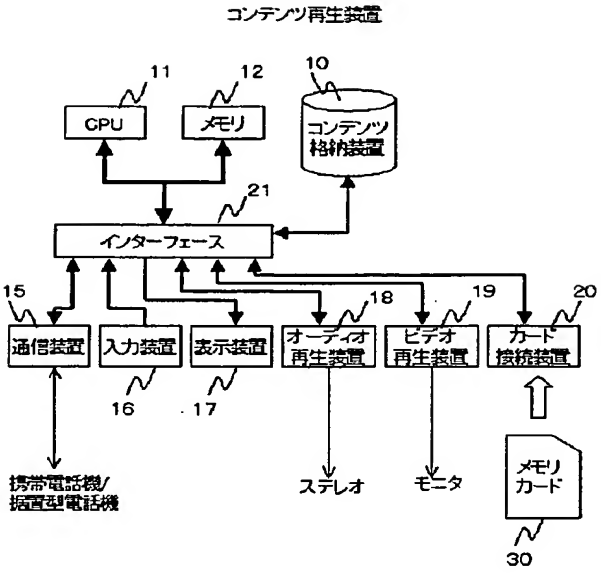
【図１１】本発明の１実施形態が適用されたコンテンツ再生装置のコンテンツ格納装置１０の鍵格納装置１０１から本コンテンツ再生装置に接続されたメモリカード３０へライセンス鍵を移動する場合の動作を説明するためのフロー図である。

【符号の説明】

１１、１０２…ＣＰＵ
１２、１０４…メモリ
１０…コンテンツ格納装置
１５…通信装置
１６…入力装置
１７…表示装置
１８…オーディオ再生装置
１９…ビデオ再生装置
２０…カード接続装置
２１…インターフェース
３０…メモリカード
４１…操作パネル
４２…受信部
４３…表示パネル
４４、４５…スロット
４６…コネクタ
５０…リモコン
５１…モニタ
５２…ステレオ
５３…携帯電話機
１０３…フラッシュメモリ
１０５、１０７、１８４、１９４…Ｉ/Ｏ回路
１８１、１９１…暗復号化回路
１８２、１９２…デコーダ回路
１９３…フレームバッファ

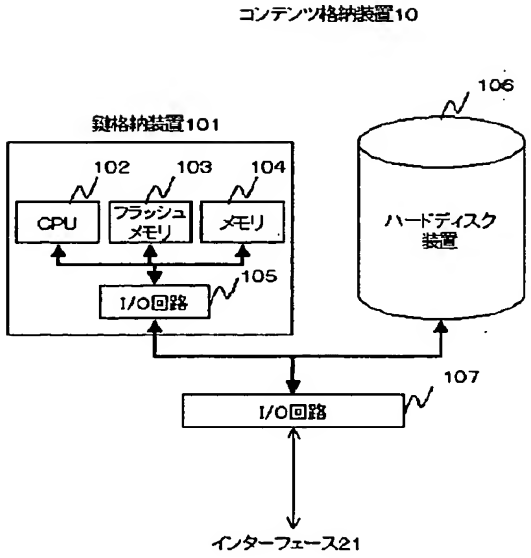
【図１】

図1



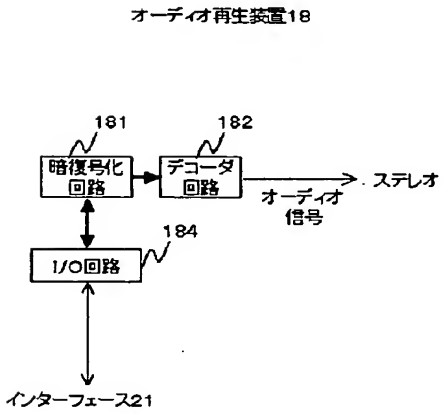
【図２】

図2



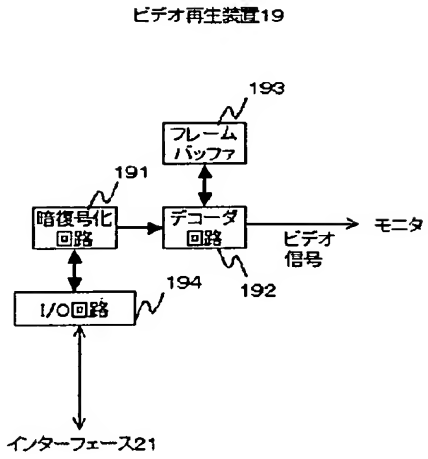
【図３】

図3



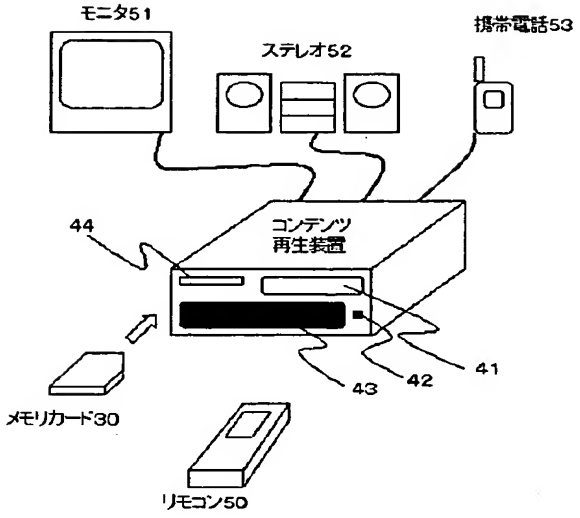
【図４】

図4



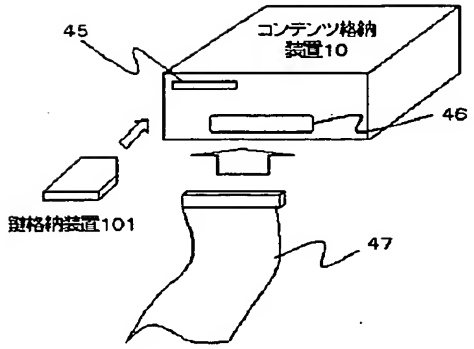
【図５】

図5



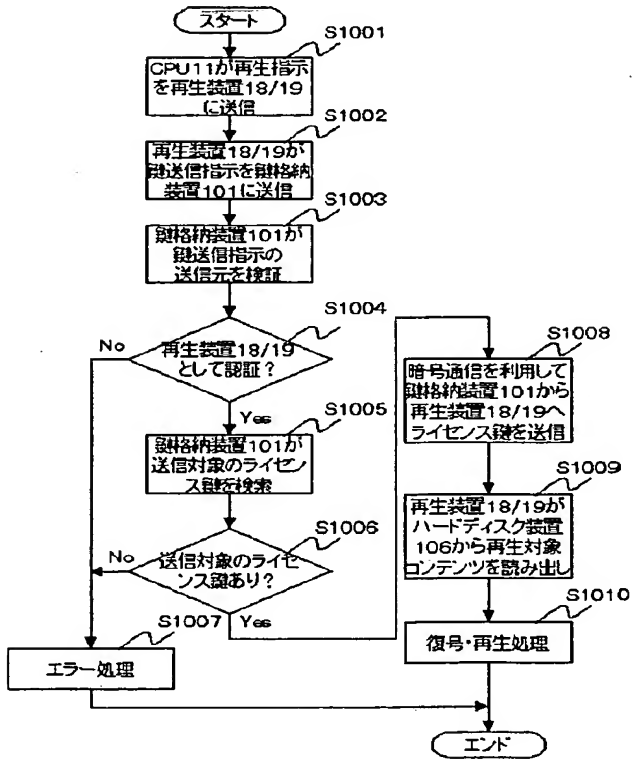
【図６】

図6



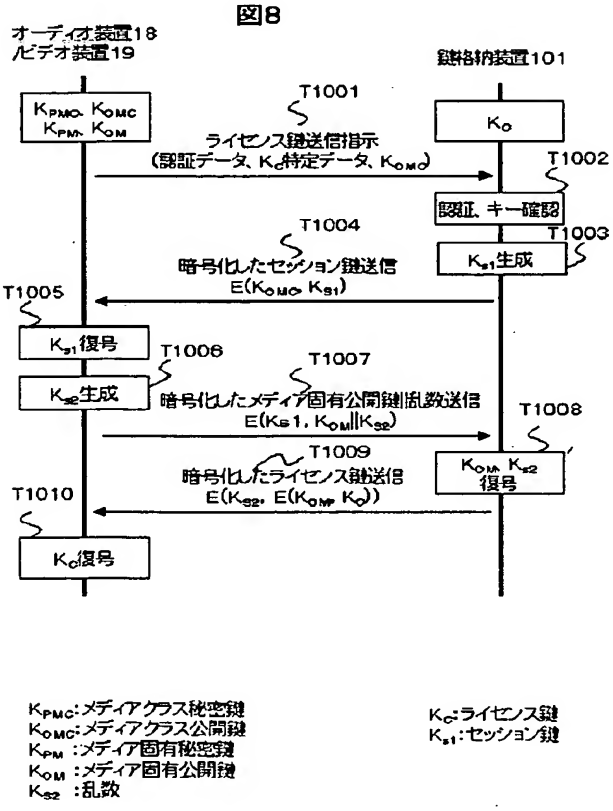
【図７】

図7



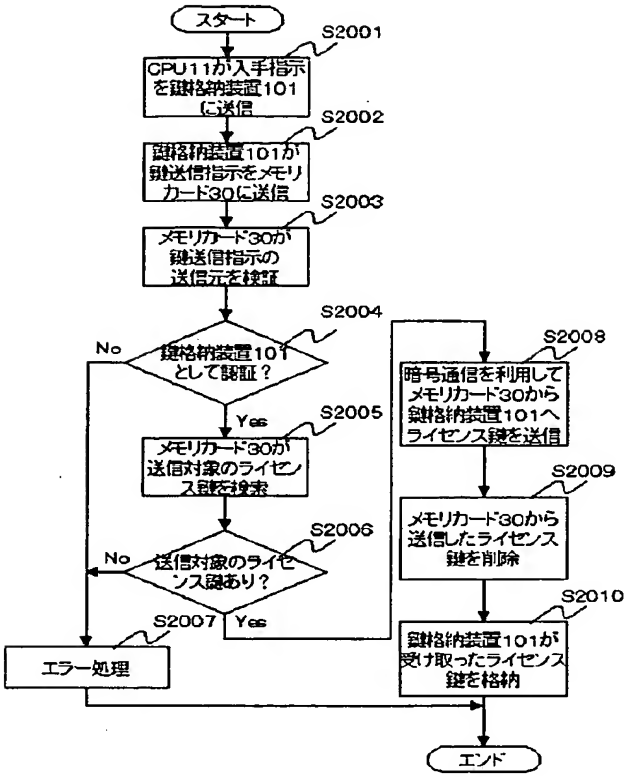
【図８】

図8



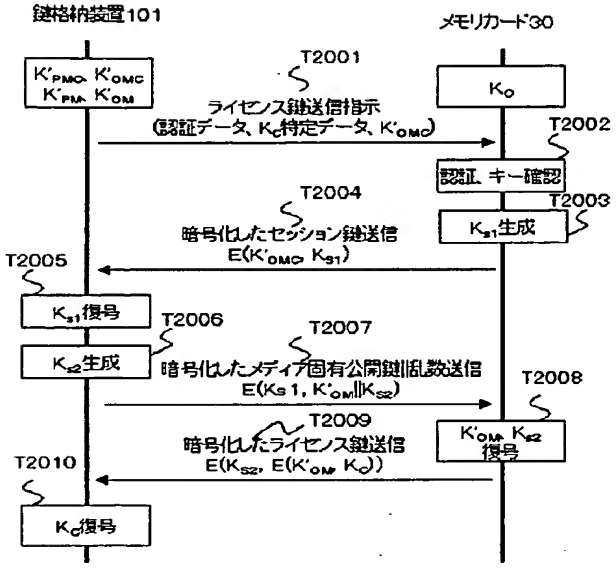
【図９】

図9



【図１０】

図10

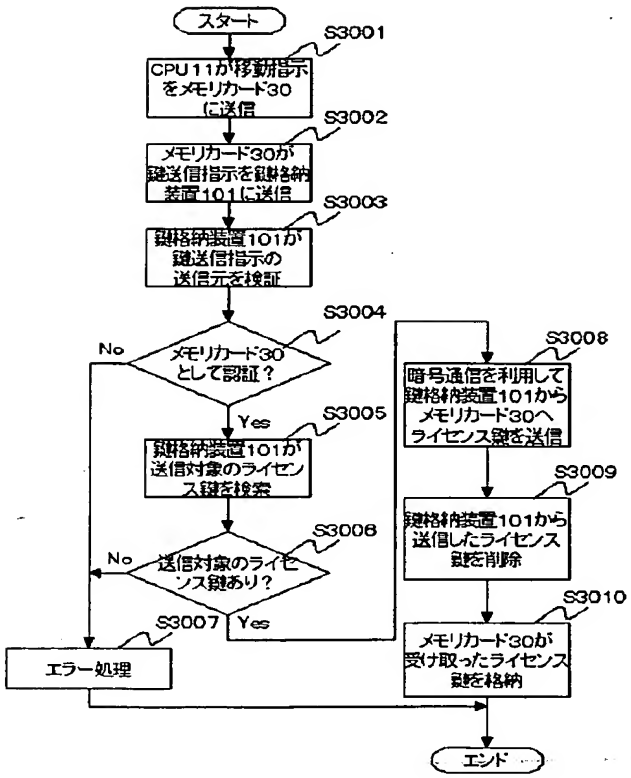


K'PMC:メディアクラス秘密鍵
K'OMC:メディアクラス公開鍵
K'PM :メディア固有秘密鍵
K'OM :メディア固有公開鍵
Ks2 :乱数

Kc:ライセンス鍵
Ks1:セッション鍵

【図１１】

図11



フロントページの続き

(51)Int.Cl.[7]		識別記号	F I			テーマコード (参考)
G09C	1/00	660	G11B	20/10	H	5C064
G11B	20/10		H04L	9/00 621	A	5D044
H04N	5/91		H04N	5/91	P	5J104
	7/167			7/167	Z	9A001

(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　角田　元泰
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　白石　和久
神奈川県小田原市国府津2880番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　戸塚　隆
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内
(72)発明者　▲真▼野　宏之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　中村　一男
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内

Ｆターム(参考)　5B017 AA06 BA07 BB03 CA07 CA14
CA16
5B058 KA01 KA04 KA06 KA33 KA35
5B075 KK07 KK50 KK54 KK63 KK68
MM01 MM11 MM23 ND16 UU37
5B085 AA01 AE00 AE09 AE29 BE01
5C053 FA13 FA15 FA23 FA27 FA29
GA11 GB21 JA01 JA21 KA24
LA11 LA14
5C064 CA14 CB01 CC02 CC04
5D044 AB05 AB07 CC08 DE50 DE53
DE58 GK12 GK17 HL08
5J104 AA12 EA06 EA09 EA18 EA19
KA02 NA02 NA03 NA35 NA37
9A001 BB03 EE03 JZ67 KK62 LL03